IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Joseph C. KAWAN et al.

Serial No.: **09/588,902** Art Unit: **3624**

Filed: **June 9, 2000** Examiner: **HAMILTON, Lalita**

For: **METHOD AND SYSTEM FOR CONTROLLING CERTIFICATE BASED ON OPEN PAYMENT TRANSACTIONS**

APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Window, Mail Stop **Appeal Brief - Patents**
Randolph Building
Alexandria, VA 22314

Sir:

This is an Appeal Brief under 37 C.F.R. § 41.37 in connection with the Final Office Action of September 12, 2005 and Notice of Appeal filed January 30, 2007. Each of the topics required by Rule 41.37 is presented herewith and is labeled appropriately.

(1) Real Party In Interest

The real party in interest is Citicorp Development Center, Inc.

(2) Related Appeals And Interferences

Appellants are unaware of any related appeals or interferences.

(3) Status Of Claims

Claims 1-15, 17-19, 22-24 and 28 are pending in the present application. Claims 1-15, 17-19, 22-24 and 28 stand under final rejection, from which rejection this appeal is taken. Claims 16, 20, 21 and 25-27 were previously canceled.

(4) Status of Amendments

The claims have not been amended after the final Office Action dated September 12, 2005.

(5) Summary Of Claimed Subject Matter

This summary of claimed subject matter is a concise explanation of the subject matter defined in independent claims 1, 22 and 28. This is merely meant to be a summary and is in no way intended to limit the pending claims. The undersigned directs the reader to and cites particular portions of the specification which describe the subject matter of the independent claims.

The text of Claims 1, 22 and 28 is set forth below with support therefore from the specification in *italics*:

1. (Previously Presented) A method for facilitating a financial transaction over a first network (***Figure 1**, reference S(C)*) comprising:

issuing a locked programmable memory device to a first user, wherein the programmable memory device contains at least the following for formulating payment instructions, network address instructions for an issuer of the programmable memory device, a first user's financial account information, and an encryption program (***Pg. 11, ll. 15-22 & Figure 3**: "In the preferred embodiments these certificates **26** may be stored in any appropriate electronic memory **23**, preferably a non-volatile reprogrammable memory such as, EEPROM or Flash, within the electronic chip **20** within the smart card **10** as well as in an optical memory **15** and/or a magnetic memory **17**, should these be available on the smart card **10**. Further, the electronic memory **23** is capable of storing other large files/programs **24** such as biometric identifying information **36**, a digital signature generation program **30**, and memo balances **38** as well as the on-card generated encryption keys **28** used to encrypt any or all of these files for security." **Pg. 13, l.27-pg. 14, l.3 & Figure 3**: "Additionally, the smart card contains the dialing number and URL for the SP, a menu for selecting which account he wishes to debit, and memo balances for informing the customer or merchant of the value amounts in each of his available accounts." **Pg. 21, ll. 16-25**: "Depending upon the security needs of the customer, in an embodiment of the present invention, the customer generates his/her own key pair off of the issued smart card, instead of receiving the generated keys with the smart card. In this embodiment, the SP issues the smart card to the customer having a standard PIN thereon for unlocking the card, but the encryption key pairs and the certificate have yet to be generated. When the customer receives the card and unlocks the card with the PIN, using the software supplied by the SP the customer is able to generate his/her own key pair and a profile to be encrypted with a digital signature based on the private key and forwarded to the SP along with the attached public key for formation of a service provider-backed certificate. A profile contains information such as name, address, social security number, birthdate, etc.");*

unlocking the programmable memory device at the first user with a first user's predetermined personal identification number (*See above on Pg. 21*);

programming the programmable memory device at the first user to include a first user identification profile and a private/public key pair using the encryption program (*See above on Pg. 21*);

issuing software to a second user, wherein the software includes payment information of the second user including a second user's financial account information and further wherein the software is capable of interacting with the programmable memory device over the first network (***Pg.14, ll. 8-12***: *"The merchant subscribes to the certificate-based open payment transaction system and has loaded the appropriate software and/or hardware into the POS terminal. This software is not complicated and in most cases need only consist of a file containing the public keys of the SP so as to be capable of decrypting, authenticating, and authorizing messages received from the SP under a PKC security system."*);

forming a connection between the programmable memory device and the software (***Pg. 12, ll. 16-20:*** *"Referring to **FIG. 5**, when attempting to make a purchase from a participating merchant, the customer inserts the smart card into an appropriate reader at a POS terminal or through a reader connected to his PC, PDA, or a wireless device (e.g., cellular phone, set-top box, or similar portable terminal) or he retrieves the certificate from his hard drive and sends it to the merchant/customer terminal **54**." Fig. 1, reference S(C); **Pg. 19, ll. 16-19:** "When the order form is complete, the customer digitally signs the purchasing information with his private key and attaches the certificate from the smart card to the purchasing information and executes the transmit step (e.g., selecting "send"), resulting in the form being sent over the network to the SP.*");

receiving across the connection the payment instructions (***Pg. 14, ll. 16-20***: *"When the customer attempts to pay through a stationary, on-line terminal using his smart card, the merchant requests payment and the customer inserts his smart card into the smart card reader portion of the merchant terminal **S2**. The reader recognizes the certificate and other purchase facilitating data in the memory or memories of the smart card." See above at **Pg. 19, ll. 16-19**)*;

adding the second user's payment information to the payment instructions (***Pg. 15, l. 25-Pg. 16, l.9***: *"After the customer has selected his method of payment and has signed the certificate with his private key, the merchant proceeds to add additional transaction data, pertaining to his payment needs to the certificate prior to sending it to the SP **S10**. This additional data may include the merchants financial institution routing number as well as the merchant's deposit account number and the merchant's encrypted digital signature for identification by the SP. Alternatively, the merchant's information is already attached to a payment vehicle prior to the customer adding his/her information as in the case of a web-based transaction." **Pg. 19, ll. 11-14**: "If the merchant is a participant in the certificate-based open payment transaction system, the merchant bank's routing number and the account therein which the merchant wishes to have credited, will automatically be added to the purchasing data entered by the customer.");*

routing the payment information and the payment instructions to an issuer utilizing the network address instructions (***Pg. 16, ll. 10-12:*** *"When the merchant has completed the addition of his data and digitally signed the certificate, the dialing number or URL on the smart card, dials up the SP and transmits all of the certificate information thereto **S11**." Fig. 1, reference S(C); **Pg. 19, ll. 16-19:** "When the order form is complete, the customer digitally signs the purchasing information with his private key and attaches the certificate from the smart card to the purchasing information and executes the transmit step (e.g., selecting "send"), resulting in the form being sent over the network to the SP.*"); and

receiving the payment information and the payment instructions, wherein the issuer is capable of accessing at least one of the first user's financial account information and a second user's financial account information (***Pg. 16, ll. 12-15***: *"Upon receiving the certificate, the SP will decrypt and authenticate the merchant's ID signature as well as the customer's ID information and authorize the customer's certificate in light of the purchase information* ***S12***." ***Pg. 17, ll. 10-13***: *"Finally, the SP will pay the merchant and post the debit to the customer's account either with the SP or with the third party financial institution* ***S19***. *The payment and posting steps may be accomplished through the traditional automated clearing house (ACH) channels.").*

22. (Original) A method for performing a financial transaction comprising:

presenting a customer with an amount due in response to a customer's product selection (***Pg. 14, ll. 16-21:*** *When the customer attempts to pay through a stationary, on-line terminal using his smart card, the merchant requests payment and the customer inserts his smart card into the smart card reader portion of the merchant terminal* ***S2***. *The reader recognizes the certificate and other purchase facilitating data in the memory or memories of the smart card. If the purchase price exceeds $1,000, biometric authentication is required and the customer will be asked to provide such information, e.g., a fingerprint* ***S3-S5***.");

accepting a customer's programmable memory device within a reader portion of a terminal to facilitate payment of the amount due (*See above at* ***Pg. 14, ll. 16-21)***;

accessing a portion of the customer's programmable memory device containing payment information, wherein the payment information includes at least network address instructions for an issuer of the customer's programmable memory device, a digital certificate for identifying the customer, the customer's financial account information, an encryption program, and a customer memo balance containing updated customer account balances (***Pg. 13, l. 17- Pg. 14, l. 7:*** *"Referring to* ***FIG. 4****, in a first specific example, a customer obtains a smart card encrypted with a certificate from the SP,* ***S1*** *and attempts to make a purchase at a POS merchant terminal. By way of example, the customer's smart card contains an identification certificate which includes the SP's digital signature that is secured on a first-level by encryption via public key cryptography (PKC) and is further secured on a second-level by a PIN lock. If necessary, a smart card could be programmed to individually lock any number of applications within the smart card with a PIN. The smart card itself may be secured by a PIN lock and/or biometric lock, adding a third and possibly, fourth level of security. The smart card could be programmed to require biometric authentication only when the customer attempts to make a purchase for value exceeding a set amount, for example $1,000. Additionally, the smart card contains the dialing number and URL for the SP, a menu for selecting which account he wishes to debit, and memo balances for informing the customer or merchant of the value amounts in each of his available accounts.*");

identifying the customer through the digital certificate ((***Pg. 14, ll. 16-20***: *"When the customer attempts to pay through a stationary, on-line terminal using his smart card, the merchant requests payment and the customer inserts his smart card into the smart card reader portion of the merchant terminal* ***S2***. *The reader recognizes the certificate and other purchase facilitating data in the memory or memories of the smart card."* ***Pg. 16, ll. 12-15***: *"Upon receiving the certificate, the SP will decrypt and authenticate the merchant's ID signature as well as the customer's ID information and authorize the customer's certificate in light of the purchase information* ***S12***.")*;*

receiving a customer's account selection (*See above at **Pg. 13, l. 17- Pg. 14, l. 7** and **Pg.15, ll. 7-9:** "Once the smart card is accessed, the customer decides which account he wishes to use for the purchase **S9**. By way of the GUI, the customer is able to review the memo balance file to aid in the selection of an account to be debited." **Pg. 18, l. 12-15**: "The customer then selects which account he wishes to use in the transaction **S21** and if necessary, the merchant is able to view the memo balances and determine the availability of funds within the customer's chosen account **S22-S24**.");*

checking a customer's memo balance for the selected account to determine if funds therein are sufficient to pay the amount due (***Pg. 18, l. 12-15**: "The customer then selects which account he wishes to use in the transaction **S21** and if necessary, the merchant is able to view the memo balances and determine the availability of funds within the customer's chosen account **S22-S24**.*");

downloading the payment information from the programmable memory device to a memory portion of the terminal (***Pg. 18, l. 17-22**: "Optionally, the merchant may utilize his own terminal and smart card for storing these off-line transactions, an audit copy of the transactions, his own identification certificates containing, for example, merchant digital signatures, and dialing numbers and URLs for appropriate financial institutions and/or SPs **S26**. The merchant may store the transactions from, for example, a single day, in aggregate or summarized form on his smart card, and in transaction specific form in the merchant terminal memory.*");

storing the payment information from the programmable memory device in a memory portion of the terminal for future processing of the financial transaction (*See above at **Pg. 18, l. 17-22***);

releasing the selected product to the customer (***Pg. 18, ll. 15-16:** "Once a viable account has been selected, the merchant releases the purchased goods and/or services to the customer **S25**.*");

uploading the payment information to the issuer of the programmable memory device for further processing and settlement of the financial transaction (***Pg. 18, ll. 22-24:** "At a time convenient for the merchant, the merchant goes on-line (e.g., direct dial or Internet) and utilizes his smart card and/or terminal to up-load batches of transactions to the SPs **S27**.*").

28. (Previously Presented) A system for facilitating a financial transaction comprising:

a programmable memory device issued to a first user including (***Figure 1**, S(A); **Figure 3***)

(a) at least one processor (***Pg. 11, ll. 15-22 & Figure 3**: "In the preferred embodiments these certificates **26** may be stored in any appropriate electronic memory **23**, preferably a non-volatile reprogrammable memory such as, EEPROM or Flash, within the electronic chip **20** within the smart card **10** as well as in an optical memory **15** and/or a magnetic memory **17**, should these be available on the smart card **10**. Further, the electronic memory **23** is capable of storing other large files/programs **24** such as biometric identifying information **36**, a digital signature generation program **30**, and memo balances **38** as well as the on-card generated encryption keys **28** used to encrypt any or all of these files for security.*");

(b) a digital certificate for identifying the user (***See above***);

(c) the user's financial account information (***Pg. 13, l.27-pg. 14, l.3 & Figure 3**: "Additionally, the smart card contains the dialing number and URL for the SP, a menu for*

selecting which account he wishes to debit, and memo balances for informing the customer or merchant of the value amounts in each of his available accounts.");

(d) network addressing instructions for at least the issuer of the programmable memory device (***Pg. 13, l.27-pg. 14, l.3 & Figure 3**: "Additionally, the smart card contains the dialing number and URL for the SP, a menu for selecting which account he wishes to debit, and memo balances for informing the customer or merchant of the value amounts in each of his available accounts."*);

(e) an encryption program for encrypting at least (b) and (c) wherein the encryption program is employed by the user after issuance of the programmable memory device thereto for generating a private/public key pair (***See above at Pg. 11, ll. 15-22 & Figure 3***); and

(f) at least one re-writable memory configured to track information related to the financial transaction (***See above at Pg. 11, ll. 15-22 & Figure 3***);

a terminal for reading information from the programmable memory device to facilitate a payment from at least one of a user's financial accounts (***Pg. 7, ll. 5-7: "The system further includes a first server for offering at least one product via the network through a terminal and a processor connected to the terminal."***);

a server for receiving information from the terminal read from the programmable memory device and authorizing payment from at least one of the user's financial accounts (***Pg. 7, ll. 13-18:*** *"A second server connected to the network for (f) receiving the encrypted payment information with the attached identifying certificate, (g) decrypting and reading the encrypted payment information with the attached identifying certificate, (h) authorizing a payment requested via the payment information, and (g) notifying the first server of the authorization."*); and

a programmable memory device issued to a second user for storing information related to the financial transaction (***Pg. 18, l. 17-22**: "Optionally, the merchant may utilize his own terminal and smart card for storing these off-line transactions, an audit copy of the transactions, his own identification certificates containing, for example, merchant digital signatures, and dialing numbers and URLs for appropriate financial institutions and/or SPs **S26**. The merchant may store the transactions from, for example, a single day, in aggregate or summarized form on his smart card, and in transaction specific form in the merchant terminal memory."*).

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1-15, 17-19, 22-24 and 28 are rejected under 35 U.S.C. 102(e) as being unpatentable over Sehr (US Publication No. 2001/0018660).

(7) Argument

In the Final Office Action, the Office incorporates its previous rejections by reference. The Office previously referred to paragraphs [0063] and [0105] of Sehr as disclosing the claim language including "adding the second user's payment information to the payment instructions; routing the payment information and the payment instructions to an issuer utilizing the network

address instructions." The undersigned rebutted this assertion, pointing out that these paragraphs failed to disclose these limitations. In the Final Office Action, the Office now points to Page 2, para. [0024] as disclosing these limitations; paragraph [0024] states:

> [0024] This invention relates to an automated admission system and methods for facilitating via a portable visitor card device a plurality of services, comprising storing admission rights, service entitlements, and cardholder considerations into the visitor card; loading monetary values and electronic payment forms in the card; issuing and using the card for admission and purchases of goods and services; rendering the services requested and clearing the payments made via the card; and communicating card data and related service information between and among the system entities.

The Office specifically recites the following with respect to the limitation directed towards "adding the second user's payment information to the payment instructions;" --- "loading monetary values and electronic payment forms in the card and clearing the payments made via the card, **which may include vendor information**." Importantly, the highlighted portion of the Office's statement is NOT actually recited in paragraph [0024]. Similarly, paragraph [0024] does not disclose "routing the payment information and the payment instructions to an issuer utilizing the network address instructions." Indeed, paragraph [0024] does not anticipate the claim language.

As previously addressed by the undersigned, the only addition to the visitor's electronic payment information is a security key – not the vendor's payment information. Further, the claim language recites "routing the payment information and the payment instructions to an **issuer**... ." (Emphasis added). Importantly, Sehr does not disclose routing any payment information or instructions to the issuer of the visitor card. In Sehr, the issuer of the visitor card and the entities who receive the payment information and instructions are not the same. (See at least FIG. 1 and paragraphs [0027] and [0028], wherein it is clear that the Admission Center (2) for "automated **issuance** of visitor cards" is distinctly different from Service Providers (3) such as "a bank or financial institution that stores an electronic monetary value or other electronic payment means in the card, a credit reporting firm that verifies and guarantees the credit worthiness of the cardholder, a transaction processor that clears and credits the electronic payments made via the card, or a certification center that authenticates cardholders and card data.") Accordingly, in addition to the limitations discussed above, Sehr also fails to disclose

"receiving the payment information and the payment instructions, wherein the **issuer** is capable of accessing at least one of the first user's financial account information and a second user's financial account information." (emphasis added). For at least these reasons, the undersigned submits that Sehr does not anticipate claim 1 or the claims dependent thereon.

As argued in the undersigned's previous response, Sehr does not disclose each and every element of claim 22. More specifically, Sehr does not disclose "storing the payment information from the programmable memory device in a memory portion of the terminal for future processing of the financial transaction," as recited in claim 22. The Office now cites to paragraph [0030] of Sehr for this teaching. Paragraph [0030] states:

> [0030] The distributed databases (10), (20) and (30) are associated with the plurality of remote system entities that comprise the event organizer, admission center and service providers, respectively. The above database scheme comprises database storage means for storing data and information in a distributed manner between and among those remote entities including the portable visitor card. The databases include the data records that relate to the entities and to the visitor card contents. Further included is information including electronic template files, which implement the card's usage and the system's operations. Also stored is card data and system information to support the communications and data security management functions. As a function of the amount and complexity of the data to be stored, this database can be implemented via a variety of storage configurations. Solid state memory, magnetic tape, rotating media, video disks, and optical/laser media, are examples thereof.

This general paragraph describing data storage does not anticipate the specific limitation set forth in claim 22. As discussed in the previous response, though Sehr arguably describes a terminal, e.g., the Card Read/Write Device, Sehr does not store payment information from the programmable memory device.

Additionally, Sehr does not disclose "uploading the payment information to the **issuer** of the programmable memory device for further processing and settlement of the financial transaction... ." (emphasis added). As discussed above with respect to claim 1, in Sehr, the issuer of the visitor card and the entities who receive, process and settle the payment information are not the same. (See at least FIG. 1 and paragraphs [0027] and [0028]). The Office now cites to paragraph [0032] for this teaching. Paragraph [0032] states:

> [0032] The EVENT ORGANIZER employs a plurality of means to compile and authenticate the card contents, communicate data between the card and system

> entities, manipulate card data and update the system databases, and to exchange information with the admission center and service providers. These means comprise the database (10), visitor card (11), card read/write device (12), biometrics box (13), computing platform (14), and various software programs to implement the application routines and network communication as instructed by the event organizer. These system components are connected via a communication link (19) to allow the exchange of data/information throughout the organizer entity. These local components, including the event organizer per se, are also connected via a global communication link (1234) to the remote system components, including the service providers and admission center. The global data link also allows the visitors to communicate with the system entities via a personal computer or card terminal installed at remote locations, such as the visitor's home, a business office, or public places.

Though this paragraph generally references communication amongst the issuer and other entities, the claim limitation is specific in its requirements, i.e., "uploading the payment information to the **issuer** of the programmable memory device for further processing and settlement of the financial transaction... ." (emphasis added). Clearly this paragraph does not anticipate this uploading step. It does not describe payment information flowing from the programmable memory device to the issuer for processing and settlement. Accordingly, Sehr does not disclose each and every element of claim 22. The undersigned representative requests that the Office withdraw the rejection of claim 22 and claims 23 and 24.

Further, Sehr does not disclose each and every element of claim 28, as previously amended. As set forth in a previous response, claim 28 was amended to further recite "a programmable memory device issued to a second user for storing information related to the financial transaction." Sehr does not disclose a vendor, merchant, or other party besides a visitor having a visitor card (11). "The Electronic Visitor Card (11) is the portable card used by the visitors when attending an event or buying goods and services." *See, e.g.*, para. [0056]. The Office again cites to paragraph [0030] (set forth explicitly above) for this teaching. The undersigned again fails to see where this paragraph anticipates the claim language? Sehr does not disclose a second user having a programmable memory device and, therefore, does not disclose each and every element of claim 28. The undersigned representative respectfully requests that the Office withdraw the rejection of claim 28.

(8) Claims Appendix

See Claims Appendix below.

(9) Evidence Appendix

None.

(10) Related Proceedings Appendix

None.

Respectfully submitted,

Date: 7/2/07

By: */Dawn-Marie Bey Reg. No.44,442/*

Dawn-Marie Bey
Registration No. 44,442

KILPATRICK STOCKTON LLP
Suite 900
607 14th Street, N.W.
Washington, D.C. 20005
(202) 508-5889

Appendix of CLAIMS

1. (Previously Presented) A method for facilitating a financial transaction over a first network comprising:

issuing a locked programmable memory device to a first user, wherein the programmable memory device contains at least the following for formulating payment instructions, network address instructions for an issuer of the programmable memory device, a first user's financial account information, and an encryption program;

unlocking the programmable memory device at the first user with a first user's predetermined personal identification number;

programming the programmable memory device at the first user to include a first user identification profile and a private/public key pair using the encryption program;

issuing software to a second user, wherein the software includes payment information of the second user including a second user's financial account information and further wherein the software is capable of interacting with the programmable memory device over the first network;

forming a connection between the programmable memory device and the software;

receiving across the connection the payment instructions;

adding the second user's payment information to the payment instructions;

routing the payment information and the payment instructions to an issuer utilizing the network address instructions; and

receiving the payment information and the payment instructions, wherein the issuer is capable of accessing at least one of the first user's financial account information and a second user's financial account information.

2. (Original) The method according to claim 1, wherein the payment information of the second user further includes a second user's digital certificate.

3. (Original) The method according to claim 1, wherein the first network is the Internet.

4. (Original) The method according to claim 1, wherein the first network is a wireless network.

5. (Original) The method according to claim 1, wherein the network address instructions include at least one of a universal resource locator and a phone number.

6. (Original) The method according to claim 1, further including authorizing a payment amount read from the payment instructions.

7. (Original) The method according to claim 6, wherein authorizing a payment amount includes requesting via a second network authorization from a first user's financial institution that maintains the first user's financial account information.

8. (Original) The method according to claim 7, wherein the payment instructions further include an encrypted personal identification number recognizable by the first user's financial institution for accessing the first user's financial account information.

9. (Original) The method according to claim 7, wherein the second network is an ATM network.

10. (Original) The method according to claim 7, wherein the second network is the Internet.

11. (Original) The method according to claim 1, wherein the programmable memory device is a smart card.

12. (Original) The method according to claim 1, wherein the first user's financial account information includes the first user's account identifier.

13. (Previously Presented) The method according to claim 12, wherein the first user's account identifier includes at least one of an account type and an account number.

14. (Original) The method according to claim 1, wherein the first user's financial account information includes the first user's financial institution routing number.

15. (Original) The method according to claim 1, wherein the encryption program contains a private key generated by the issuer.

16. (Cancelled)

17. (Previously Presented) The method according to claim 1, wherein the second user's financial account information includes the second user's account identifier.

18. (Original) The method according to claim 17, wherein the second user's account identifier includes at least one of an account type and an account number.

19. (Original) The method according to claim 1, wherein the second user's financial account information includes the second user's financial institution routing number.

20.-21. (Cancelled)

22. (Original) A method for performing a financial transaction comprising:

presenting a customer with an amount due in response to a customer's product selection;

accepting a customer's programmable memory device within a reader portion of a terminal to facilitate payment of the amount due;

accessing a portion of the customer's programmable memory device containing payment information, wherein the payment information includes at least network address instructions for an issuer of the customer's programmable memory device, a digital certificate for identifying the customer, the customer's financial account information, an encryption program, and a customer memo balance containing updated customer account balances;

identifying the customer through the digital certificate;

receiving a customer's account selection;

checking a customer's memo balance for the selected account to determine if funds therein are sufficient to pay the amount due;

downloading the payment information from the programmable memory device to a memory portion of the terminal;

storing the payment information from the programmable memory device in a memory portion of the terminal for future processing of the financial transaction;

releasing the selected product to the customer;

uploading the payment information to the issuer of the programmable memory device for further processing and settlement of the financial transaction.

23. (Original) The method according to claim 22, wherein the terminal is wireless.

24. (Original) The method according to claim 22, further comprising:

receiving verification from the issuer of the programmable memory device that the financial transaction is authorized; and

updating a merchant transaction log in the memory portion of the terminal to reflect authorization of the financial transaction by the issuer of the programmable memory device.

25-27. (Cancelled)

28. (Previously Presented) A system for facilitating a financial transaction comprising:

a programmable memory device issued to a first user including

(a) at least one processor;

(b) a digital certificate for identifying the user;

(c) the user's financial account information;

(d) network addressing instructions for at least the issuer of the programmable memory device;

(e) an encryption program for encrypting at least (b) and (c) wherein the encryption program is employed by the user after issuance of the programmable memory device thereto for generating a private/public key pair; and

(f) at least one re-writable memory configured to track information related to the financial transaction;

a terminal for reading information from the programmable memory device to facilitate a payment from at least one of a user's financial accounts;

a server for receiving information from the terminal read from the programmable memory device and authorizing payment from at least one of the user's financial accounts; and

a programmable memory device issued to a second user for storing information related to the financial transaction.